Information Security in IT Contracting

Joshua G. Kuntz CISSP (ISC)²

Information Security Officer

Texas Department of Motor Vehicles

Objectives

- Understand your Security Policies
- Know your business
- Ensure Security is included in the SDLC process
- Include Security Elements in Contracts

Understand your Security Policies

Texas Cybersecurity Framework - 44 controls based on NIST 800.53

- IT Contracting Controls
  - External vendors and Third-Party Providers
  - Secure System Services, Acquisition, and Development
  - Third-Party Personnel Security
- Additional Controls to consider
  - Data Classification and Privacy & Confidentiality
  - Privacy/Security Awareness & Training
  - Cloud Usage and Security
  - Secure Application Development and Vulnerability & Penetration Testing
  - Cybersecurity/Privacy Incident Response
  - Continuity Planning & Disaster Recovery Procedures

Cloud Service Providers

- Cloud Service Providers can offer excellent opportunities to provide enterprise level solutions for many functions. However, not all Cloud Services are created equal.
- Ensure your security and legal teams are involved in user license agreement/contract reviews. Many Providers operate outside of the US where laws and regulations are significantly different.
- Quantify the impact of service outages and select providers based on their stated and proven ability to meet those expectations.

Secure Application Development

- Establish Coding Standards and Measurements
  - Use one or more established code quality standards to define the expectation (Consortium for IT Software Quality, Open Web Application Security Project, Center for Internet Security, etc…)
  - Define a code quality check interval and minimum quality standard
- Vulnerability Assessment & Penetration Testing
  - All online or mobile applications that process any sensitive personally identifiable or confidential information must undergo testing prior to deployment and remediate all findings (TGC§2054.516)

Know your Business

- Use the Business Impact Analysis
  - Maps organizational functions to state and federal essential functions
  - Articulates criticality of organizational functions
  - Denotes disaster recovery priorities and timelines
- Understand the Data Classification of the proposed system
  - Is the data exempt from public release? (TGC§552)
  - Are there additional statutory or industry protections (HIPPA, FTI, PCI…)?
- Understand the Risk Appetite of your Organization
  - How much operational downtime is acceptable?
  - Does that downtime appetite change in the event of a disaster?

Ensure Security is Included in the SDLC

- Define Cybersecurity Deliverables in the Project Initiation Phase
  - System/Data Security Plans
  - System and Data Flow Diagrams
  - Network and Interconnection Diagrams
  - Disaster Recovery and Continuity Plans
  - Vulnerability & Penetration Tests
- Ensure Security is Part of the Scoring Matrix for Contract Award
  - Service Providers should submit a copy of their information security policies for comparison to organizational policies
  - Security “Track Record” (Incidents and Incident Responses) should be considered in Reference Checks

Include Security Elements in Contracts

- **Security Clauses**
  - Contractor Background Checks
  - Confidentiality Non-Disclosure
  - Adherence to Security Policies
  - Incident Response & Notification
  - System Documentation
  - System & Data Security Plans
  - Disaster Recovery Plans & Testing
- **Coding Clauses**
  - Code Quality Expectations
    - Measurement Methodology
  - Code Ownership & Escrow
  - Vulnerability & Pen Tests
    - Findings' Remediation
    - Retest Requirements
  - System Up Time Requirement
    - Measurement Interval
    - Measurement Exclusions

Contact Information

Joshua G. Kuntz CISSP(ISC)²

joshua.Kuntz@txdmv.gov